REMARKS

Claims 1-7, 10-17 and 20-30 are pending in this application.

In the Office Action, claims 1, 5 and 14 and all dependent claims to claims 1, 5 and 14 have been rejected under 35 U.S.C. § 112, first paragraph. Claims 5 and 14 and all dependent claims to 5 and 14 have been rejected under 35 U.S.C. § 112, second paragraph. Claims 1-7, 10-17 and 20-30 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,950,195 (Stockwell et al.) in view of U.S. Patent No. 6,304,973 (Williams).

35 U.S.C. § 112 Rejections

Claims 1, 5, 14 and all dependent claims 1, 2, 5, and 14 have been rejected under 35 U.S.C. § 112 first paragraph. Applicant respectfully traverses theses rejections.

Initially, Applicant notes that the Examiner seems to be confused and not understand the limitations in the claims of the present application. Applicant finds this somewhat surprising since this is at least the fourth Office Action issued in this case by the same Examiner where these claims and these limitations have been examined. It appears that after having examined these claim limitations many times before and issued previous Office Actions with art rejections, the Examiner now claims to not understand the limitations in the present claims and asserts these 35 U.S.C. § 112 rejections. Applicant respectfully requests that the Examiner re-assign this case to another Examiner if the present Examiner is uncomfortable with the technology related to the claims of the present application.

Further, the limitations in the claims of the present application are clearly supported and enabled in Applicant's specification and drawings. The firewall, FTP proxy, file system, and database are clearly shown in figure 2. Further, the remaining limitations are clearly disclosed and illustrated in figure 3 and Applicant's disclosure.

The Examiner states that the claims have been rejected based on the specific limitation "the user who uses "Anonymous" is permitted to use only commands other than the commands for file transmission to an external network", which is recited in Applicant's disclosure on page 14 at the end of paragraph [46]. Applicant fails to see why the claims of the present application are rejected based on this disclosure in Applicant's detailed description. For the Examiner's understanding, the limitations in the claims of the present application relate to checking an ID of an internal user if the received service command is a command requesting data transmission. Further, if the user ID is "anonymous" the transmission of the received service command (i.e., requesting data transmission) is interrupted and not sent to the external network. This is completely consistent and enabled by the statement that the Examiner refers to that recites "the user who uses "Anonymous" is permitted to use only commands other than the commands for file transmission to an external network". This is further supported in Applicant's figure 3, reference characters ST20, ST21 and ST22, and paragraph 46 starting on page 13 that discloses that if the received command is "STOR", which is used for transmitting files to the FTP server in the external network, the FTP proxy determines whether the user ID is "anonymous" and if so, prevents the command from being transmitted to the FTP server. Applicant submits that the

limitations in the claims of the present application are fully enabled in Applicant's specification and drawings.

For the Examiner's better understanding, Applicant refers the Examiner to figure 3 of Applicant's application. As shown in this figure, when an access to connect with the server is requested, ST13, it is determined whether the user is anonymous and if so, the user is connected to the server, ST16. Otherwise, access control occurs, ST15. Further, once a user (anonymous or otherwise authorized) is connected to the sever, an anonymous user is prevented from transmitting data to the server, ST20-22, whereas other connected users are allowed to transmit data and the information related to the transmission logged in a file, ST21, ST23-ST25. Applicant hopes that this clarifies the Examiner's understanding of the present application.

Accordingly, Applicant respectfully requests that these rejections be withdrawn and that these claims be allowed.

Claims 5 and 14 and all dependent claims 2, 5, and 14 have been rejected under 35 U.S.C. § 112 second paragraph. Applicant respectfully traverses these rejections.

Regarding claim 5, the Examiner asserts that the phrase "the server" on line 14 lacks antecedent basis. However, this claim has an antecedent basis from the phrase "a server" in line 6 of claim 5.

Regarding claim 14, the Examiner asserts that the phrase "the server" on line 14 lacks antecedent basis. The Examiner further asserts that "it needs to be external server/external

network." Applicant respectfully disagrees with these assertions. The term "the server" has antecedent basis in claim 14, line 7.

Accordingly, Applicant respectfully requests that these rejections be withdrawn.

35 U.S.C. § 103 Rejections

Claims 1-7, 10-17 and 20-30 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Stockwell et al. in view of Williams. Applicant respectfully traverses these rejections.

Stockwell discloses regulating the flow of internetwork connections through a firewall having a network protocol stack which includes an Internet Protocol (IP) layer. A determination is made of the parameters characteristic of a connection request, including a netelement parameter characteristic of where the connection request came from. A query is generated and determination is made whether there is a rule corresponding to that query. If there is a rule corresponding to the query, a determination is made whether authentication is required by the rule. If authentication is required by the rule, an authentication protocol is activated and the connection is activated if the authentication protocol is completed successfully.

Williams et al. discloses a network that prevents unauthorized users from gaining access to confidential information. The network has various workstations and servers connected by a common medium and through a router to the Internet. The network has two major components, a Network Security Center (NSC) and security network interface cards or devices. The NSC is an administrative workstation through which the network security officer manages

the network as a whole as well as the individual security devices. The security devices are interposed, between each of workstation, including the NSC, and the common medium and operate at a network layer (layer 3) of the protocol hierarchy. The network allows trusted users to access outside information, including the Internet, while stopping outside attackers at their point of entry. At the same time, the network limits an unauthorized insider to information defined in their particular security profile. The user may select which virtual network to access at any given time. The result is trusted access to multiple secure Virtual Private Networks (VPN), all from a single desktop machine.

Regarding claims 1, 5, 14 and 23, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose suggest or render obvious the limitations in the combination of these claims. For example, the Examiner asserts that Stockwell et al. discloses wherein the FTP proxy determines whether or not an ID transmitted from an internal user of the internal network is a registered ID, at col. 7, line 45- col. 8, line 29. However, these portions merely disclose that access control list rules are checked in sequential order and that the position of the rule is the sole criteria for determining whether or not the rule is selected, and that a sanity check is performed to warn the administrator if a rules position is obviously wrong, and that once a rule is selected the agent receives a reply that can allow or deny the connection and provides explanations. This is not wherein an FTP proxy determines whether or not an ID transmitted from an internal user of the internal network is a registered ID, as recited in the claims of the present application. Stockwell et al. merely relates to whether a rule corresponds to

a query and determining whether authentication is required by the rule. Stockwell et al. does not disclose or suggest determining whether an ID is a registered ID.

Further, the Examiner asserts that Stockwell discloses where access control is not performed if the ID transmitted from the internal user is "anonymous" such that the internal user is permitted to connect to a server located in the external network without access control, at col.12, lines 23-44. However, these potions merely disclose two rules in a rule set where a first rule allows any client in the internal security domain to access any FTP server in the external domain and the second rule supports an anonymous FTP server on the local firewall. This is not access control not being performed if the ID transmitted is "anonymous" allowing a user to connect to the external network, as recited in the claims of the present application. These portions disclose that any client in the internal security domain can access any FTP server in the external domain, and merely that an anonymous FTP server is supported on the local firewall. This is not related to access control not being performed based on an ID transmitted being "anonymous".

The Examiner further asserts that Stockwell et al. discloses checking an ID of the internal user if the received service command is a command requesting data transmission, if the user is "anonymous" interrupting the transmission of the received service command to the external network, and if the user ID is a registered ID other than " anonymous" transmitting the received service command to the external network and transmitting the data received from the internal user to the external network, at col. 9, lines 16-31 and 34-39. However, these portions merely

disclose details related to figure 4 of Stockwell et al. regarding information included in a prompt for a user name, that a second access control list check should be performed, and should include the same parameters as the first check plus the name of the user and the selected warder (special server performing the authentication), and that if the reply to the second check is denied, the connection is dropped, else the reply will include a list of allowed warders for that user if the reply to the checks is allowed. This is not checking an ID of an internal user if the received service command is a command requesting data transmission, as recited in the claims of the present application. Further, these portions do not disclose or suggest interrupting the transmission of the received service command to the external network if the user ID is "anonymous", or transmitting the received service command to the eternal network and transmitting the data from the internal user to the external server if the user ID is a registered ID other than "anonymous". These portions in Stockwell et al. merely disclose details that an agent goes through in authenticating a connection.

Regarding claims 2-4, 6, 10-13, 15-17, 20-22 and 24-30, Applicant submits that these claims are dependent on one of independent claims 1, 5, 14 and 23 and, therefore, are patentable at least for the same reasons noted previously regarding these independent claims.

Accordingly, Applicant submits that none of the cited references, taken alone or in any proper combination, disclose suggest or render obvious the limitations in the combination of each of claims 1-7, 10-17 and 20-30 of the present application. Applicant respectfully requests that these rejections be withdrawn and that these claims be allowed.

CONCLUSION

In view of the foregoing remarks, Applicant submits that claims 1-7, 10-17 and 20-30 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested. If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the undersigned attorney, Frederick D. Bailey, at the telephone number listed below.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this, concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
FLESHNER & KIM, LLP

Daniel Y.J. Kim
Registration No. 36,186
Frederick D. Bailey
Registration No. 42,282

P.O. Box 221200
Chantilly, Virginia 20153-1200
(703) 766-3701 DYK/FDB:tlgknh
Date: AUGUST 15, 2006
Please direct all correspondence to Customer Number 34610

\\Fk4\Documents\2000\2000-084\94737.doc